PACTO

Pembrokeshire Association of Community Transport Organisations
Cymdeithas Mudiadau Cludiant Cymunedol Sir Benfro

PACTO Data Protection Policy

1. Scope

This policy applies to staff, volunteers, services and service users of services provided *directly* by the charity known as Pembrokeshire Association of Community Transport Organisations. Other community transport services and schemes which operate within Pembrokeshire are governed by their own policies and procedures.

2. Overview and Definitions

2.1 Wherever PACTO collects or uses personal or sensitive personal data, we act in accordance with the General Data Protection Regulations, EU Regulation 2016/679 (hereafter referred to as GDPR)

2.2 The GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2.3 **Definitions:**

Personal Data is defined as information from which you can identify an individual person, for example name, address, phone number, email address or photograph of the person.

Sensitive Personal Data is defined as information concerning a person's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

The person whose data is collected is called the "Data Subject"

3. Responsibilities

3.1 PACTO is not required by law to appoint a Data Protection Officer.

3.2 The Trustees are responsible for ensuring overall compliance with GDPR through establishing and monitoring this policy. Day-to-day responsibility for the implementation of this policy will sit with PACTO's Manager. Staff and volunteers handling information are made aware of their responsibilities regarding the collection, use and sharing of personal data on behalf of PACTO.

4. Lawful basis for Collecting Information

4.1 The GDPR provides six valid lawful bases on which personal data can be processed:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

4.2 In practice, most personal data collected and processed by PACTO is covered by **"Legitimate Interest"**, because (a) people would reasonably expect us to collect their data, for example so that we can provide them with a service such as Bus Buddies or MiDAS Training, and/or (b) we are required to collect the information in order to meet reporting obligations to our funders.

4.3 On occasion, we will need to seek **Consent** for the collection of personal information and/or use in different ways which would not be covered by Legitimate Interest. For example, for marketing and promotional communications, or use of photographs for publicity purposes.

5. Data Audit

5.1 We will identify, for all areas of our work:
- What personal data we collect
- The lawful basis under GDPR which entitles us to collect this information
- Where and how the information is stored
- How long the information is retained for
- Who it is shared with
- Any risks and risk mitigation factors.

5.2 When planning a new area of work which will require the processing of personal date, we will carry out a Privacy Impact Assessment, using the same headings as above, in order to plan data protection measures from the outset.

6. Collecting Personal Data and Privacy Notices

6.1 As a general principle, we will seek to collect the minimum personal data required to carry out our work and to fulfil any contractual requirements (e.g. reporting to our funders).

6.2 Whenever we collect personal data, we will provide Data Subjects with a Privacy Notice, which explains:
- who we are;
- under what lawful basis we are collecting their personal information
- what we are going to do with their information; and
- who their information will be shared with (if anyone).

6.3 Wherever practical, privacy notices will be incorporated into the relevant forms.

6.4 Where a Data Subject does not complete the form themselves (e.g. assistance is provided by a PACTO member of staff or volunteer) or data is collected through other means (e.g. over the telephone) the Privacy Notice will be provided verbally.

6.5 It may occasionally be appropriate to provide the Privacy Notice on a notice or sign, for example if we are conducting a survey at an event such as the County Show.

7. Consent

7.1 Where Consent is required, we will normally get confirmation in writing. The consent form will include details of how to withdraw consent.

7.2 We will keep clear records of who has given Consent. We will act promptly on any requests to withdraw consent.

7.3 Any mail-outs or marketing communications will include clear information about who to contact if someone wishes to withdraw their consent.

8. Storage and Retention of Personal Data

8.1 Whether in hard copy or electronically, we will take steps to ensure that Personal Data is stored securely:
- Hard Copies will be stored in locked cupboards.
- Electronic information will be stored in password protected or encrypted files

8.2 We will not keep data for longer than necessary. This will be identified as part of the Data Audit.

8.3 We are aware of the need to dispose of personal data securely. Hard copies will be shredded. We will take reasonable precautions to ensure Personal Data is removed from PACTO IT equipment prior to disposal.

9. Sharing Information with Others

9.1 PACTO works closely with partner organisations to deliver many of our services. This will sometimes require us to share Personal and Sensitive Personal Data about our clients to ensure that they get the service they require.

9.2 We will normally **only** share Personal Data with others where we have a lawful basis to do so, and where this has been explained to the Data Subject in the Privacy Notice.

9.3 On rare occasions, where we have legitimate safeguarding concerns, we may share Personal Data with other organisations without prior notice. For further information see PACTO's Vulnerable Adult Protection Policy.

9.4 Where necessary, we will put in place Data Sharing Agreements with key partners and contractors. These Agreements will clearly define the role and responsibilities of both parties in relation to the Personal Data, in particular which Organisation has the role of Data Controller (with ultimate responsibility), and which is the Data Processor.

9.5 We will take proportionate steps to ensure that Personal Data is shared *securely*, for example through the use of encrypted emails. This will also apply when Personal Data is shared internally between PACTO Staff and/or Volunteers.

10. Subject Access Requests

10.1 Under GDPR, individuals have the right to obtain confirmation that their data is being processed; access to their personal data; and information about how and why we are using their personal data (i.e. the information provided in the Privacy Notice).

10.2 We will respond to all Subject Access Requests within one month, unless the request is complex or numerous in which case this may be extended to up to three months.

10.3 We will take reasonable steps to verify the identity of the person making the request.

11. Right to Erasure and Restriction

11.1 Individuals have the right to have their personal data erased if:

- (Where we are relying on consent as our lawful basis for holding the data) the individual withdraws their consent;
- (Where we are relying on legitimate interests as our lawful basis) the individual objects to the processing of their data, **and** there is no overriding legitimate interest to continue this processing;

11.2 Individuals also have the right to request that their personal data be restricted or suppressed.

11.3 If we have disclosed the personal data to others, we will contact each recipient and inform them of the erasure or restriction, unless this proves impossible or involves disproportionate effort.

12. Emails and Other Electronic Communication

12.1 The GDPR covers Personal Data stored and sent via email or other electronic communication (such as Text Message or Social Media). Any emails or messages containing unsecured Personal Data should be deleted and/or securely archived once they have been dealt with.

12.2 Any Personal Data sent via email **by** PACTO staff or volunteers should be sent securely (i.e. via Encrypted Files) or should be anonymised (for example non-identifying details sent via email, with an accompanying phone call to provide the remaining information).

13. Home Working and Working out of the Office

13.1 As a general rule, all Personal Data should usually be kept securely in the office. However, the nature of PACTO's work means that staff and volunteers are often required to work out and about in the community and/or from home, and this may require them to take Personal Data with them.

13.2 Staff and volunteers will be permitted to take Personal Data out of the office, for the purpose of carrying out specific duties such as a visit to a prospective client in order to complete the Registration Form. The Staff and Volunteers concerned should *only* carry the minimum information they require with them (i.e. just the form for that individual and not the whole registration file), and any personal information should be securely destroyed or returned to the Office at the earliest opportunity.

13.3 Staff working from home should discuss with their Line Manager any potential Data Protection issues and take reasonable precautions to ensure the security of any Personal Data processed outside of the office.

13.4 Personal Data should never be processed or sent from unsecured WiFi hotspots.

14. **Use of Personal Devices**

14.1 It will sometimes be appropriate for PACTO staff and volunteers to use their own personal devices (e.g. mobile phone, home computer) to receive Personal Data on behalf of PACTO, e.g. Bus Buddy volunteers might be given contact details for a Service User, Project Staff may take photographs of volunteers or clients on behalf of PACTO.

14.2 Any such Personal Data remains the property of PACTO and must NEVER be shared with others, including on personal social media, without express permission from your Line Manager. Personal Data on staff and volunteers' personal devices should be deleted as soon as it is no longer required. Any information collected when out and about, e.g. photographs, should be transferred to PACTO's own computer system as soon as reasonably practical and deleted from the personal device immediately.

14.3 When a staff member or volunteer leaves the organisation, we will take reasonable steps to ensure that any Personal Data belonging to PACTO has been removed from their personal devices.

14.4 Where staff or volunteers are required to access or process large amounts of Personal Data, frequently, out of the office, consideration will be given to providing them with a PACTO mobile phone, laptop or tablet computer and/or to storing the information on a secure remotely accessible system, such as DropBox.

14.5 Staff and volunteers using personal devices to store and access Personal Data on behalf of PACTO will be required to enable basic security features on their device, such as screen locking with password or PIN protection.

15. Data Breaches

15.1 A personal data breach is an accidental or deliberate breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. For example:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

15.2. Some personal data breaches will not pose any risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect the individuals whose personal data has been compromised, for example by causing emotional distress or physical and material damage.

15.3 On becoming aware of a breach, we will take steps to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

15.4 We will document all breaches, including any resulting actions we have taken. We will notify the Information Commissioner's Office (ICO) within 72 hours of any data breach which is likely to cause a risk to people's rights and freedoms.

15.5 Where we are processing data on behalf of another organisation, we will notify them of any breach as soon as reasonably possible.

15.6 If a breach is likely to affect the individuals whose Personal Data has been compromised, we will inform those concerned as soon as reasonably possible.

16. Monitoring and Review

16.1 We will review the policy periodically to take into account changes in legislation or in PACTO's activities. The policy will be reviewed as a matter of course every two years.

Signed on behalf of the Trustee Board.....

Date...14/5/18.....

Signed on behalf of the Trustee Board.....

Date...14/05/2018...